

REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the present amendment in the following discussion is respectfully requested.

Claims 1-10 and 12-30 are presently pending in this case. Claims 1, 17, 23, 27, and 28 are amended and new Claims 29 and 30 are added by the present amendment. As amended Claims 1, 17, 23, 27, and 28 and new Claims 29 and 30 are supported by the original disclosure,¹ no new matter is added.

In the outstanding Official Action, Claims 1-10, 12-25, 27, and 28 were rejected under 35 U.S.C. §103(a) as unpatentable over Ishiguro et al. (U.S. Patent Application Publication No. 20020194475, hereinafter “Ishiguro”) in view of Noguchi et al. (U.S. Patent Application Publication No. 20020023216, hereinafter “Noguchi”); and Claim 26 was rejected under 35 U.S.C. §103(a) as unpatentable over Ishiguro in view of Noguchi and further in view of Akkermans et al. (U.S. Patent Application Publication No. 20060104449, hereinafter “Akkermans”).

With regard to the rejection of Claims 1, 17, 23, 27, and 28 as unpatentable over Ishiguro in view of Noguchi, that rejection is respectfully traversed.

Amended Claim 1 recites in part:

wherein ***said authenticating means provides device identification data identifying the device to be authenticated, master key data, original key data, and service identification data to said key generating means***, said service identification data including first service identification data corresponding to a first service to be received by a user of the device to be authenticated and second service identification data corresponding to a second service to be received by the user of the device to be authenticated, said key generating means selects one of said first service identification data or said second service identification data, said key generating means selects a key generation algorithm corresponding to selected service identification data from among a plurality of different key generation algorithms, and ***said key generating means***

¹See, e.g., the specification at paragraphs 33, 64, and 65 of the publication.

generates said key data by inputting the device identification data, the master key data, the original key data, and the selected service identification data into said selected key generation algorithm.

As noted in the present specification at paragraph 65, by generating key data based on all of the device identification data, the master key data, the original key data, and the selected service identification data, the claimed invention provides greater security because even if one or more of these items is compromised, security can be maintained as at least one remains secret. Further, basing the key data on these four items provides flexibility in allowing different users to freely change the original key data while maintaining overall security for other users due to the secrecy of the other data unchanged by the user.

The outstanding Office Action cited the generation of keys sk1' and sk2' of Ishiguro as "key data" as recited in Claim 1, and cited paragraph 77 of Noguchi as describing the use of different key generation algorithms.² Ishiguro describes that keys sk1' and sk2' are based only on two items, the license key and the session key. Further, paragraph 106 of Ishiguro also describes that the license key lk1 is computed by subjecting a concatenation of a device ID and the service key to a hash function. Thus, Ishiguro does not appear to describe key generating means that generates said key data by inputting ***the device identification data, the master key data, the original key data, and the selected service identification data*** into said selected key generation algorithm. Therefore, Ishiguro does not teach "key generating means" as defined in amended Claim 1.

Noguchi describes a communication verification system which generates a symmetric key Kc based only on random number R.³ Accordingly, Noguchi also does not appear to describe key generating means that generates said key data by inputting ***the device identification data, the master key data, the original key data, and the selected service***

²See page outstanding Office Action at page 3.

³See Noguchi, paragraph 75.

identification data into said selected key generation algorithm. Therefore, Noguchi also does not teach “key generating means” as defined in amended Claim 1. Further, even combining the key generation of Noguchi and Ishiguro would not provide key generating means that generates key data based on all the claimed data.

Thus, as the proposed combination does not teach or suggest “key generating means” as defined in amended Claim 1, Claim 1 (and Claims 2-16 dependent therefrom) is patentable over Ishiguro in view of Noguchi.

Amended Claims 17 and 23 recite in part “said generating including generating said key data by inputting *the device identification data, the master key data, the original key data, and the selected service identification data* into said selected key generation algorithm.”

As noted above, Ishiguro describes that keys sk1' and sk2' are based only on two items, the license key and the session key. Ishiguro also describes that the license key lk1 is computed by subjecting a concatenation of a device ID and the service key to a hash function. Noguchi describes that symmetric key Kc is based only on random number R. Further, even combining the key generation of Noguchi and Ishiguro would not provide generating key data based on all the claimed data. Therefore, the proposed combination does not teach “generating” as defined in amended Claims 17 and 23. Consequently, Claims 17 and 23 (and Claims 18-22 and 24-26 dependent therefrom) are also patentable over Ishiguro in view of Noguchi.

Amended Claim 27 recites in part:

said key generating circuit generates said key data by inputting *the device identification data, the master key data, the original key data, and the selected service identification data* into said selected key generation algorithm.

Again, Ishiguro describes that keys sk1' and sk2' are based only on two items, the license key and the session key. Ishiguro also describes that the license key lk1 is computed

by subjecting a concatenation of a device ID and the service key to a hash function. Noguchi describes that symmetric key Kc is based only on random number R. Further, even combining the key generation of Noguchi and Ishiguro would not provide a key generating circuit that generates key data based on all the claimed data. Therefore, the proposed combination does not teach “a key generating circuit” as defined in amended Claim 27. Consequently, Claim 27 is patentable over Ishiguro in view of Noguchi.

Amended Claim 28 recites in part:

said key generating unit is configured to generate said key data by inputting *the device identification data, the master key data, the original key data, and the selected service identification data* into said selected key generation algorithm.

Ishiguro describes that keys sk1' and sk2' are based only on two items, the license key and the session key. Ishiguro also describes that the license key lk1 is computed by subjecting a concatenation of a device ID and the service key to a hash function. Noguchi describes that symmetric key Kc is based only on random number R. Further, even combining the key generation of Noguchi and Ishiguro would not provide a key generating unit that generates key data based on all the claimed data. Therefore, the proposed combination does not teach “a key generating unit” as defined in amended Claim 28. Consequently, amended Claim 28 is patentable over Ishiguro in view of Noguchi.

With regard to the rejection of Claim 26 as unpatentable over Ishiguro in view of Noguchi and further in view of Akkermans, it is noted that Claim 26 is dependent from Claim 23, and thus are believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Akkermans does not cure any of the above-noted deficiencies of Ishiguro and Noguchi. Accordingly, it is respectfully submitted that Claim 26 is patentable over Ishiguro in view of Noguchi and further in view of Akkermans.

Finally, new Claims 29 and 30 are supported at least by the specification at paragraph 33. As new Claims 29 and 30 are dependent from Claim 1, these claims define over Ishiguro

Application No. 10/791,760
Reply to Office Action of December 15, 2008

in view of Noguchi for at least the reasons described above with respect to Claim 1.

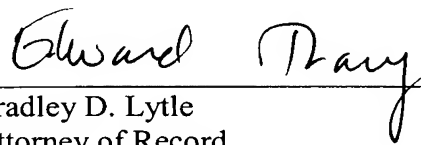
Accordingly, new Claims 29 and 30 are also allowable.

Accordingly, the pending claims are believed to be in condition for formal allowance.

An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

A handwritten signature in cursive script, appearing to read "Bradley D. Lytle", is written over a horizontal line.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

Edward W. Tracy, Jr.
Registration No. 47,998

683774_1.DOC